UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

information associated with dbanks451@gmail.com and the accounts of dbanks@icloud.com and dbanks451@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc. more fully described in Attachment A

Case No. 19-854M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:
Title 18, United States Code, Section 1591(a) (sex trafficking by force, fraud, or coercion)

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Todd P. Higgins, TFO
Applicant's signature

Todd P. Higgins, TFO
Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 8, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Todd P. Higgins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a deputized Federal Task Force Officer (TFO), with the United States Department of Justice, Drug Enforcement Agency, currently assigned to DEA Group 68, at the North Central High Intensity Drug Trafficking Area (HIDTA). I was deputized as a TFO with the DEA in 2018. In addition to being a TFO with the DEA, I have been a Special Agent with the Wisconsin Department of Justice, Division of Criminal Investigations (DCI) since 2014. Prior to my employment for DCI, I was a Detective for the City of Brookfield Police Department and I have been in law enforcement for over 18 years. My responsibilities as a TFO include the investigation of violent crimes, criminal enterprises, violations relating to the illegal sale and transfer of narcotics and firearms, and violent criminal acts in furtherance of criminal enterprises. In addition, my duties include the investigation of drug trafficking organizations and violations of federal narcotics and money laundering laws, including, but not limited to offenses defined by 21 U.S.C. § 841, 843, and 846, and 18 U.S.C. § 1956. I have received further specialized

training concerning the interception of wire and electronic communications. I have also have training in regards to human trafficking and have worked such cases, at both the State and Federal level, for approximately 2 years.

3. The lead investigator for this investigation is Special Agent Melissa A. Fus. Agent Fus is a Special Agent with the Wisconsin Department of Justice-Division of Criminal Investigation (DOJ-DCI) and has been in law enforcement since 2003. Agent Fus is currently assigned to the Human Trafficking Bureau for the Wisconsin Department of Justice and also the Federal Bureau of Investigation Wisconsin Human Trafficking Task Force ("WHTTF"). Agent Fus's duties as a Special Agent with the WI DOJ-DCI include human trafficking investigations involving minors and adults. Agent Fus has gained experience in the conduct of such investigations through previous case investigations, formal training, and in consultation with law enforcement partners in local, state, and federal law enforcement agencies. I have discussed this case with Agent Fus.

4. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider to be truthful and reliable. Some of the information was provided in response to administrative subpoenas and search warrants, and I believe that this information is also reliable.

5. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, instrumentalities, and/or fruits

of violations of Title 18, United States Code, Section 1591(a) (sex trafficking by force, fraud, or coercion), as described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. Human Trafficking of AV-2

1. Special Agent Melissa Fus participated in interviews with an adult female (hereinafter referred to as AV-2) (DOB XX/XX/1991). AV-2 disclosed that she met Darren Hatchett II (DOB XX/XX/1985) in November 2008 in Indiana. AV-2 stated that sometime in 2010 or 2011, AV-2 began engaging in prostitution at Hatchett's direction.

2. In October 2011, AV-2 was interviewed by officers at the Anaheim Police Department in California. AV-2 stated to those officers that she and Hatchett left Indiana in approximately July 2011 and that shortly thereafter Hatchett instructed her on how to conduct prostitution activities. AV-2 stated she gave Hatchett all the money she made from those activities. A-2 stated that she was never allowed to keep any of the money and that if she wanted anything to eat or drink, she had to ask him for money.

3. AV-2 told Anaheim officers that Hatchett hit her all the time, that he choked her frequently and that, on at least one occasion, he choked her to the point where she passed out.

4. AV-2 stated to Anaheim officers that Hatchett and AV-2 traveled to Costa Mesa, California, with another adult victim (hereinafter referred to as AV-5) (DOB XX/XX/1990). AV-

2 stated that because she was pregnant, Hatchett stopped posting her for prostitution dates and started posting AV-5. AV-5 also gave all the money she earned from prostitution activity to Hatchett.

5. While in Buena Park, California, in the fall of 2011, Hatchett began choking and hitting AV-2 while they were driving. AV-2 escaped by jumping out of the car, and Hatchett pulled her back in by her hair. During this encounter, AV-2 was helped by a man who took her to the police station. After this incident, AV-2 returned to Indiana and gave birth to Hatchett's child.

6. Based on interviews with AV-2 and others, AV-2 returned to Hatchett in 2015. AV-2 stated that after she returned to Hatchett in 2015 she lived with him in a house at 3411 W. Clybourn Street, in Milwaukee (hereinafter referred to as "Hatchett's Residence"). She remained living in Hatchett's Residence until she left Hatchett in May 2018. AV-2 believed Hatchett owned the house. AV-2 stated that Hatchett would sometimes lock the house to prevent her from leaving, and that he had multiple cameras set up in the interior and exterior of the house.

7. She again engaged in prostitution at his direction and gave the money she earned from prostitution activity to Hatchett. Hatchett continued to be violent toward AV-2. In 2015, Hatchett broke AV-2's jaw and she had to have it wired shut for approximately six weeks. AV-2 stated that Hatchett's violence toward her was a regular occurrence. Hatchett hit her in the head with guns. On at least two occasions he broke her skull and caused bleeding. He also dragged her down the stairs, hit her with an electrical cord all over her body, hit her with the handle of a mop or broom, shot at her, and locked her in a dog kennel in a bedroom. While she was in the kennel, Hatchett threatened to shoot her. These instances of abuse, including the shooting, primarily occurred at Hatchett's Residence.

8. AV-2 reported that Hatchett possessed several firearms, which he eventually stored in a large safe at his residence on Clybourn. Those firearms included handguns and assault rifles. At one point, Hatchett gifted AV-2 an assault rifle that he had customized. When AV-2 left Hatchett in May 2018, she did not take the firearm with her. Even after the rifle was gifted to her, the firearm remained at Hatchett's Residence.

9. In addition to physical violence, Hatchett regularly threatened to harm AV-2's family if she left him and verbally abused AV-2 by calling her stupid and telling her that her brain was messed up.

10. During her time with Hatchett, AV-2 became addicted to Percocet. According to AV-2 and others, Hatchett withheld opioids from AV-2 as punishment if she did not do what he wanted. He also used Percocet as a reward or incentive to get her to engage in prostitution for his financial benefit.

11. AV-2 stated that during the time she was with Hatchett she traveled to multiple states, including Arizona, California, Illinois, Texas, New York, Virginia, and Colorado to engage in prostitution.

12. Multiple other victims and witnesses provided statements to law enforcement about Hatchett and AV-2. Those statements are consistent with AV-2's reports to law enforcement.

13. Record searches of websites commonly used for prostitution revealed ads for prostitution by AV-2 in Dallas, Kansas City, Virginia, Louisiana, Denver, Milwaukee, Manhattan, South Carolina, and Pennsylvania.

14. AV-2 stated that she travelled out of state with other women who also engaged in prostitution activity for Hatchett's financial gain. She identified other adult victims hereinafter referred to as AV-1 (DOB XX/XX/1997), AV-3 (DOB XX/XX/1999), AV-4 (DOB

XX/XX/1997), and AV-6 (DOB XX/XX/1994), as women who worked for Hatchett. AV-2 stated that the state she went to most frequently was Texas.

15. A search of flight records confirm AV-2's statements. For example, AV-1 and AV-2 flew from Chicago to Dallas on flights purchased by Hatchett on May 5, 2017, May 25, 2017, and October 25, 2017. On May 5, 2017, AV-6 also flew with AV-1 and AV-2. On May 30, 2017, AV-1 and AV-2 were the subject of a police report in Irving, Texas, in which the police officers noted evidence of prostitution in the hotel room in which AV-1 and AV-2 were staying. On April 23, 2018, and April 27, 2018, AV-2 and AV-3 flew to Denver and back on flights paid for by Hatchett.

16. AV-2 stated that she gave all of the money she earned from prostitution to Hatchett. AV-2 stated that when she traveled out of state, she would send Hatchett the money made from her prostitution activities by depositing the money in Hatchett's bank accounts. AV-2 stated that when she was in Texas, she deposited money into Hatchett's bank accounts.

17. AV-2 also stated that she would sometimes use services such as GoBank and Bluebird to transfer money to Hatchett at gas stations and Wal-Mart.

18. AV-2 stated that she never had her own money or bank accounts. AV-2 stated that when she decided to leave Hatchett, she secretly sent some of the money she earned to her mother. She stated that she was scared of what Hatchett would do if he found out, but that she needed to do so to avoided being stranded with her children.

19. In May 2018, AV-2 left Hatchett and moved back to Indiana. She had no money. Hatchett has continued to threaten AV-2 and has been physically abusive toward her on at least one occasion since she left him.

B. Human Trafficking of AV-5.

20. Special Agent Melissa Fus participated in interviews with AV-5. AV-5 disclosed that she met Hatchett online in 2011 and that on August 26, 2011, Hatchett and AV-2 picked her up in Indiana and drove to Indianapolis. AV-5 believed that she was going to be dancing in a gentleman's club. But when they arrived in Indiana, AV-5 learned that Hatchett intended that she engage in prostitution. In Indianapolis, AV-5 engaged in prostitution for the first time and gave all the money she earned to Hatchett.

21. AV-5 conducted prostitution activities for Hatchett's financial gain for approximately the next four years.

22. During that time, Hatchett controlled every aspect of AV-5's life. For example, Hatchett decided what cities they traveled to and when. Hatchett also decided whether, when, and for how long AV-5 was allowed to visit with family. Hatchett also controlled AV-5's social media accounts.

23. Hatchett's only source of income was the money made by AV-5 and others engaging in prostitution for his benefit.

24. AV-5 stated that starting in 2015, she and Hatchett resided at Hatchett's Residence. They continued to reside there until AV-5 left Hatchett in July 2018. Utilities at Hatchett's Residence were registered to AV-5 in April 2015. As of March 1, 2019, the utilities were in Hatchett's name.

25. AV-5 stated that Hatchett was often violent with her. The violence occurred on a regular basis and included Hatchett choking her, breaking her nose, hitting her with guns, shooting at her, pushing her down the stairs, and picking her up by the throat and throwing her to the floor. Much of this violence occurred at Hatchett's Residence. AV-5 reported that Hatchett's Residence

had bullet holes in the walls where Hatchett shot at her and other victims. AV-5 reported that she saw Hatchett shoot at AV-3 in the basement of Hatchett's Residence.

26. AV-5 reported that Hatchett possessed several firearms including assault rifles and that he has a CCW permit. AV-5 reported that Hatchett stored the firearms in a large safe in his residence on Clybourn.

27. AV-5 also became addicted to opioids and Hatchett would use that addiction to further control her by, among other things, withholding those opioids as punishment and causing AV-5 to experience withdrawal symptoms.

28. AV-5 described traveling to a variety of cities and states to engage in prostitution at Hatchett's direction and control. Flight records show that Hatchett and AV-5 flew to Dallas in March and April 2015. Hotel records show that AV-5 often rented hotel rooms in Dallas in 2013 and 2014.

29. AV-5 also identified other victims of Hatchett's human trafficking, including AV-1, AV-2, AV-4, and AV-6.

30. AV-5 left Hatchett in July 2018. AV-5 left with no money despite the fact that she estimates she made over a $1,000,000 for him. Hatchett has continued to threaten AV-5 and her family by phone.

C. Human Trafficking of AV-1

31. In July 2018, Special Agent Melissa Fus was contacted by Pewaukee Police Department regarding information on AV-1.

32. Pewaukee Police Sergeant Wright indicated that on July 14, 2018, his agency had contact with AV-1 and her family. At the time of the contact, AV-1's family reported that AV-1

was a victim of Human Trafficking and the family was attempting an intervention with AV-1. AV-1 attempted to evade the intervention and the Pewaukee Police Department was called.

33. Pewaukee Police Department officers described AV-1 as emaciated and having narcotic withdrawal symptoms. They determined that AV-1 had outstanding warrants and she was taken into custody. AV-1's family reported that Hatchett, living at Hatchett's Residence, was soliciting AV-1 for prostitution. AV-1's mother reported that AV-1 was a victim of a Human Trafficking ring in Milwaukee and AV-1 has contacted her family members several times to help her get out of the situation. AV-1's mother also told Pewaukee officers that AV-1's boyfriend, Hatchett, was very abusive and possessive. AV-1's mother also told the Pewaukee Police Department officers that AV-1 had a drug addiction. AV-1's mother also advised Pewaukee officers that there were other possible female victims who were at Hatchett's residence, in Milwaukee.

34. During AV-1's contact with Pewaukee Police Department officers, she disclosed that she resided with a group of girls. AV-1 commented that "she was just happy to be away from the house and out of the situation". AV-1 also told officers that she had not eaten for several days.

35. Special Agent Melissa Fus conducted interviews with AV-1's mother and sister. Both indicated to officers that they were aware, based on statements by AV-1, that there were multiple females who reside with Hatchett and conduct prostitution activities for Hatchett.

36. AV-1's mother said she knew of another female, AV-2, who AV-1 was frequently with. AV-1's mother indicated that AV-2 has child(ren) with Hatchett but she recently left Hatchett and returned to Indiana.

37. AV-1's mother also told officers that she knew AV-1 travelled to various states including Texas and New York to engage in prostitution activities for Hatchett.

38. A forensic examination of AV-1's phones showed numerous communications between AV-1 and male individuals that were consistent with AV-1 conducting prostitution activities. These conversations show that AV-1 was engaging in prostitution in multiple states including, but not limited to, Texas, California, and New York. The phone also contained many messages between AV-1 and Hatchett in which Hatchett and AV-1 discussed AV-1's "quota" for prostitution activities and in which Hatchett repeatedly threatened extreme violence against AV-1 and her family. For example, on March 1, 2018, Hatchett threatened to "rape yo mom and brothers" and "kill yo granny and sister with a meat cleaver." On another occasion he threatened to beat her head.

39. During interviews with AV-1, AV-1 stated that she engaged in prostitution while working for Hatchett. AV-1 stated that she was first introduced to Hatchett by another male, Brian Pointer (DOB XX/XX/1993). According to a police report from November 2011, Pointer was Trenell Henning's, Hatchett's relative's, foster son. AV-1 stated that she met Pointer on social media and that he recruited her to "work" with him and his girlfriend, AV-4. Records of AV-1's Facebook account corroborate AV-1's statements that she was initially recruited for prostitution by Pointer who told AV-1 that he and AV-4 were making money while traveling.

40. AV-1 stated that she moved in with Pointer (to Hatchett's Residence) in mid-February 2017. AV-1 said that after moving into that house, she engaged in prostitution at Pointer's direction and gave all the money she made to Pointer. AV-1 said that shortly after she moved into Hatchett's Residence she traveled to Texas with Pointer and they met AV-4 there. AV-4 and AV-1 engaged in prostitution in Texas and gave the money they made to Pointer. AV-1 flew back to Milwaukee for a court hearing on February 24, 2017. After that she went back to stay at Hatchett's residence, but Pointer was not allowed to return. Shortly thereafter, AV-1 began

engaging in prostitution for Hatchett and giving him all the money she made. AV-1 believes that Hatchett did not let Pointer return to the house because Hatchett wanted to control AV-1 and the money she made.

41. AV-1 stated that shortly after she began engaging in prostitution activities for Hatchett's financial benefit, AV-4 also began working for Hatchett.

42. AV-1 disclosed that she provided all the money she earned from her prostitution encounters after February 2017 to Hatchett. AV-1 also admitted that Hatchett controlled every aspect of AV-1's life, including who she was allowed to interact with in person and on her social media account. AV-1 also said that Hatchett dictated the cities and states to which she travelled to engage in prostitution activities. AV-1 stated that Hatchett was often violent with her and provided examples, including that on multiple occasions Hatchett choked her and on at least one occasion he shot at her with a firearm at Hatchett's residence. AV-1 disclosed that Hatchett kept a number of firearms in the residence on Clybourn. Most recently, the firearms were stored in a large safe in the residence.

43. During these interviews, AV-1 identified photographs of other victims of Hatchett's human trafficking. Those identifications included, but were not limited to AV-2, AV-3, AV-4, AV-5, and AV-6. AV-1 discussed Hatchett's violence against his victims, particularly AV-2. AV-1 also discussed how Hatchett controlled the number of pills that AV-2 consumed.

44. AV-1 also talked about her out-of-state travel with the other victims, including AV-2, and their transmittal of all of the money they made from prostitutions dates to Hatchett via bank accounts and other wire transactions. AV-1 reported that she estimates she made $500,000 from prostitution activity while working for Hatchett. When she left Hatchett in July 2018, she had no money.

45. Special Agent Melissa Fus obtained jail calls from the Waukesha County Jail made by AV-1 while AV-1 was incarcerated. The jail calls were dated from July 14, 2018, to November 18, 2018. AV-1 made frequent outgoing phone calls to Hatchett during the above dates. AV-1 frequently called Hatchett "Daddy." Based upon my training and experience, individuals who engage in human trafficking commonly require that the women who engage in prostitution activities for them call them "Daddy."

46. When AV-1 talked to Hatchett on the jail phone, she would occasionally talk to other females who were with Hatchett.

47. During some of the jail calls, Hatchett told AV-1 that he was out-of-state. For example, on November 11, 2018, Hatchett told AV-1 that he just left California and was headed to Denver. Hatchett also told AV-1 that he had been out of town for almost one month, since the day after he visited AV-1 in jail. According to AV-1's visitor log, Hatchett visited AV-1 at the Waukesha County Jail on September 18, 2018. On November 18, 2018, AV-1 asked Hatchett "You back?" and Hatchett replied, "Hell no." Hatchett said he left one light on in the house (the one when you "first walk in") so it didn't "look dead in that motherfucker."

48. During a jail call with Hatchett on October 31, 2018, Hatchett told AV-1 that he could access and control the Facebook accounts of AV-4 and AV-6.

49. AV-1 stated that Hatchett also had access to, and could control, her Facebook account when she was with him. AV-1 stated that Hatchett had control over the account when she went to jail in mid-July 2018. On July 30, 2018, Hatchett (using AV-1's Facebook account) message L.V. and to recruit L.V. to work with AV-1. During that conversation, L.V. wrote that she was threatened by AV-3, but got along with AV-4. Hatchett responded that "Daddy will make her put all that to the side I promise u that" and told L.V. to text "406-7364." That number belongs

to Hatchett. L.V. subsequently asked "Do you get to keep your money and stuff or like half and half or all of it goes to your daddy" and the Facebook account for AV-1 responded: "I'm pretty sure u know the answer to that but I guess it's cute to test the water lol."

D. Human Trafficking of AV-3, AV-4, and AV-6 and Execution of Search Warrants.

50. During a jail call with Hatchett on October 31, 2018, Hatchett told AV-1 that he could access and control the Facebook accounts of AV-4 and AV-6.

51. During interviews with AV-1 as recently as April 2019, AV-1 stated that Hatchett was traveling with AV-4, AV-6, and AV-3.

52. On February 23, 2019, AV-5 told law enforcement that Hatchett told AV-5 that he was in California with AV-3, AV-4, and AV-6.

53. Since February 2019, law enforcement has been obtaining prospective location data for Hatchett's phone, (414) 406-7364. Those records reflected that during March and April 2019, Hatchett had been in the Los Angeles area, San Francisco area, and Denver.

54. In April 2019, law enforcement obtained location data for AV-4's and AV-6's phones. That data showed that during the month of April, AV-4 and AV-6's phones were in the same areas as Hatchett. Prostitution ads posted online for AV-4 and AV-6 during this time also showed them in the same areas as Hatchett's phone.

55. As of April 18, 2019, Hatchett's phone, AV-4's phone, and AV-6's phone were in Iowa City, Iowa.

56. As of about 12:30 p.m. on April 19, 2019, Hatchett's phone, AV-4's phone, and AV-6's phone were travelling together from Davenport, Iowa to Illinois on Interstate 88.

57. On April 19, 2019, at approximately 3:00 p.m., Hatchett was arrested driving a Volvo car with California license plates. AV-3, AV-4, and AV-6 were passengers in the Volvo. Incident to Hatchett's arrest, law enforcement officers recovered a loaded firearm from the driver's seat area of the Volvo. The firearm was under the driver's seat with a portion of the firearm in plain view. The firearm is further described as a REX Zero 1CP 9mm handgun, bearing serial number A09660. During his post-arrest interview, Hatchett admitted that the 9mm handgun was his.

58. Since Hatchett's arrest, AV-3, AV-4, and AV-6 provided statements to police. During those statements, AV-3, AV-4, and AV-6 made disclosures consistent with those of AV-1, AV-2, and AV-5. AV-3, AV-4, and AV-6 admitted to engaging in prostitution activities for Hatchett's financial gain. They stated that they gave all of the money they earned from prostitution activities to Hatchett, and provided extensive details of Hatchett's consistent violence and intimidation toward them.

59. On the day after Hatchett's arrest, April 20, 2019, Hatchett called 414-795-6309 from the Waukesha County jail. On that call, Hatchett appeared to be speaking with his father, Darren Hatchett, Sr. During that call, Hatchett provided his father with his icloud account information, telling him that the account was either dbanks451@gmail.com or dbanks451@icloud.com. Hatchett asked his father to tell "Tree", who is known to be Trenell Henning (a relative of Hatchett's), to log into the account and restore it to factory settings. Hatchett told his father to "basically erase" everything on his phones. On the same day, Hatchett also called his wife, Whitney Parr-Chesser. During that call he provided her with the same iCloud account information and password and also asked her to take the phone back to "default" or "factory"

settings. On a subsequent call with Parr-Chesser, Parr-Chesser told Hatchett she had been unable to restore the icloud account, but was able to set the phone to "lost".

60. On May 1, 2019, Special Agent Melissa Fus participated in an interview with AV-6. AV-6 stated that Hatchett saved photographs, text messages, and screen shots meticulously. AV-6 stated that the text messages, pictures, and screen shots Hatchett showed Hatchett's sex trafficking activities, violence, and threats.

61. Given these statements, there is probable cause to believe that evidence of Hatchett's violations of 18 U.S.C. 1591(a) will be found on Hatchett's iCloud account.

62. Hatchett's requests to his family to delete his iCloud account provides additional reason to believe that

E. Additional iCloud Account Information/Preservation

62. On February 5th, 2019, Special Agent Melissa Fus conducted an interview with AV-5. During that interview AV-5 indicated that Hatchett had multiple email accounts/addresses. AV-5 provided an icloud email address of dbanks451@icloud.com and also the email address of dbanks451@gmail.com.

63. On February 15, 2019, Special Agent Melissa Fus sent a preservation request to Apple Inc., for the account of dbanks451@icloud.com and has since extended that preservation request.

64. On May 3, 2019, Special Agents Melissa Fus and Raymond Taylor conducted an interview with a witness named Joanne Sabir. Sabir was the previous home owner of the residence located at 3411 W. Clybourn Street, Milwaukee. Hatchett purchased the residence from Sabir with cash. Sabir reported that she primarily had contact with Hatchett via email. Sabir checked her phone and provided officers with the email address for Hatchett as dbanks@icloud.com.

INFORMATION REGARDING APPLE ID AND ICLOUD[1]

65. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

66. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be

purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

67. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

68. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

69. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

70. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

71. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

72. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

73. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

74. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. For example, these communications and files may include, among other things, text messages or screen shots of text messages between Hatchett and his victims, records of Hatchett's posting of ads for prostitution, records of financial transactions of proceeds from Hatchett's sex trafficking crimes, and photographs evidencing his control, violence, and sex trafficking activities. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of the kind of criminal activity described herein, including to communicate and facilitate the offenses under investigation.

75. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

76. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

77. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators, or applications used to post ads for prostitution, conduct financial transactions with proceeds of sex trafficking, and/or make reservations for travel and hotels used for sex trafficking activities. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

78. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including, but not limited to, information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

79. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with dbanks451@gmail.com and the accounts of dbanks@icloud.com and dbanks451@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from January 1, 2011 to the present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account January 1, 2011 to the present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All activity and transactional logs related to attempts to erase or restore the account or devices connected to the account to factory settings;

h. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

i. All records pertaining to the types of service used;

j. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

k. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within **7 days** of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and/or instrumentalities of violations of 18 U.S.C. §1591(a) involving Darren D. Hatchett II since January 1, 2011, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence of sex trafficking by means of force, fraud, or coercion;

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

g. Evidence of communications between the subscriber and his victims;

h. Evidence of the subscriber's violence toward and coercion and control of his victims;

i. Evidence indicating how and where the subscriber spent and stored the proceeds of his illegal sex trafficking;

j. Evidence of the execution of the subscriber's criminal activity, including but not limited to, records of his travel with his victims or his reservations of travel arrangements for his victims.